JC17 Rec'd PCT/PTO 16 JUL 2001

FORM-PTO-1390 (Rev. 12-29-99) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

ATTORNEY'S DOCKET NUMBER: 032326-150

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

U.S. APPLICATION NO. (If known, see 37 C.F.R. 1.5): Unassigned 09/889362

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/FR99/02918	25 November 1999	14 January 1999

TITLE OF INVENTION: PUBLIC AND PRIVATE KEY CRYPTOGRAPHIC METHOD

APPLICANT(S) FOR DO/EO/US: Pascal PAILLIER

JUL 16 2001 PATENT & TRADEMARK OFFICE

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.

2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.

3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and the PCT Articles 22 and 39(1).

4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.

5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))

   a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).

   b. ☒ has been transmitted by the International Bureau.

   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US)

6. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2)).

7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))

   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).

   b. ☐ have been transmitted by the International Bureau.

   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.

   d. ☒ have not been made and will not be made.

8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).

9. ☐ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).

10. ☒ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern other document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.

12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.

13. ☒ A FIRST preliminary amendment.

    ☐ A SECOND or SUBSEQUENT preliminary amendment.

14. ☐ A substitute specification.

15. ☐ A change of power of attorney and/or address letter.

16. ☐ Other items or information:

U.S. APPLICATION NO. (If known, see 37 C.F.R. 1.5)	INTERNATIONAL APPLICATION NO	ATTORNEY'S DOCKET NUMBER
Unassigned 09/889362	PCT/FR99/02918	032326-150

17. ☒ The following fees are submitted:	CALCULATIONS	PTO USE ONLY
Basic National Fee (37 CFR 1.492(a)(1)-(5)):		
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO $1,000.00 (960)		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO $860.00 (970)		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO $710.00 (958)		
International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy provisions of PCT Article 33(1)-(4) $690.00 (956)		
International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4) $100.00 (962)		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 860.00	
Surcharge of **$130.00 (154)** for furnishing the oath or declaration later than 20 ☐ 30 ☐ months from the earliest claimed priority date (37 CFR 1.492(e)).	$ -0-	

Claims	Number Filed	Number Extra	Rate		
Total Claims	20 -20 =	-0-	X$18.00 (966)	$ -0-	
Independent Claims	1 -3 =	-0-	X$80.00 (964)	$ -0-	
Multiple dependent claim(s) (if applicable)			+$270.00 (968)	$ -0-	
TOTAL OF ABOVE CALCULATIONS =				$ 860.00	
Reduction for 1/2 for filing by small entity, if applicable (see below).				$ -0-	-
SUBTOTAL =				$ 860.00	
Processing fee of **$130.00 (156)** for furnishing the English translation later than 20 ☐ 30 ☐ months from the earliest claimed priority date (37 CFR 1.492(f)). +				$ -0-	
TOTAL NATIONAL FEE =				$ -0-	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00 (581)** per property +				$ -0-	
TOTAL FEES ENCLOSED =				$ 860.00	
				Amount to be: refunded	$
				charged	$

a. ☐ Small entity status is hereby claimed.

b. ☒ A check in the amount of $ 860.00 to cover the above fees is enclosed.

c. ☐ Please charge my Deposit Account No. 02-4800 in the amount of $_____ to cover the above fees. A duplicate copy of this sheet is enclosed.

d. ☐ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 02-4800. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

James A. LaBarre
BURNS, DOANE, SWECKER & MATHIS, L.L.P.
P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

SIGNATURE

James A. LaBarre
NAME

28,632
REGISTRATION NUMBER

Patent
Attorney's Docket No. 032326-150

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	)	
	)	
Pascal PAILLIER	)	Group Art Unit: Unassigned
	)	
Application No.: Unassigned	)	Examiner: Unassigned
	)	
Filed: July 16, 2001	)	
	)	
For: PUBLIC AND PRIVATE KEY CRYPTOGRAPHIC METHOD	)	

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Prior to examination and the calculation of filing fees, kindly amend the above-identified application as follows:

IN THE SPECIFICATION:

Page 1, immediately following the title appearing on line 1, insert the following:

--This disclosure is based upon, and claims priority from French Application No. 99/00341, filed on January 14, 1999 and International Application No. PCT/FR99/02918, filed November 25, 1999, which was published on July 20, 2000 in a language other than English, the contents of which are incorporated herein by reference.

Background of the Invention--

Page 6, delete lines 13 and 14.

Page 6, before line 15, insert the following heading:

--**Brief Description of the Drawings**--.

Page 7, before line 4, insert the following heading:

--**Detailed Description**--.

Add the following Abstract:

--The invention concerns a cryptographic method for generating public keys and private keys. Two distinct first numbers p and q, of neighbouring value are selected, and the number n equal to the product of p.q is calculated. The lowest common multiple of the numbers (p-1) and (q-1) $\lambda(n) = PPCM(p-1, q-1)$ is then calculated. A number g, $0 < g \leq n^2$, is then determined which verifies the two following conditions: a) g is invertible modulo n^2; and b) $ord(g,n^2) = 0 \bmod n$. The public key is formed by the parameters n and g and its private key is formed by the parameters p, q and $\lambda(n)$or by the parameters p and q. An encryption method for a number m representing a message, $0 \leq m < n$, involves calculating the cryptogram $c = g^m \bmod n^2$.--

IN THE CLAIMS:

Kindly replace claims 1-20, as follows.

1. (Amended) A cryptographic method for generating public and private keys in a device that is able to exchange messages on at least one communication channel, the private key being stored secretly in said device and the public key being broadcast publicly, the generation method comprising the following steps:

- selecting two prime numbers p and q which are distinct and of similar sizes;

- calculating the number n equal to the product of p and q;

- calculating the lowest common multiple of the numbers (p-1) and (q-1): $\lambda(n)=LCM(p-1, q-1)$

- determining a number g, $0 \leq g < n^2$, which satisfies the following two conditions during the calculation of a cryptogram c, where $c=g^m \bmod n^2$:

a) g is invertible modulo n^2, and

b) $ord(g,n^2) = 0 \bmod n$, and

- selecting g = 2 if g satisfies said conditions a) and b);

wherein the public key of said device is formed by the parameters n and g and its private key is formed by at least the parameters p and q.

2. (Amended) A cryptographic communication system with public and private keys generated according to Claim 1, comprising a communication channel and first and second communicating devices, each device comprising at least one communication interface, data processing means and storage means, wherein an encryption method is

implemented in said first device to send a number m representing a message, $0 \leq m < n$, to said second device, said encryption method comprising the following steps:

- using the parameters of the public key of the second device to assign the values of the public key to the parameters n and g,

- calculating the cryptogram $c = g^m \bmod n^2$, and

- transmitting said cryptogram over the communication channel to the second device.

3. (Amended) A system according to Claim 2, wherein said first device implementing the encryption method also comprises a generator for a random integer number r, and wherein said first device:

- performs the drawing of a random integer number r, and

- calculates the cryptogram c by performing the encryption calculation: $c = g^{m+nr} \bmod (n^2)$.

4. (Amended) A system according to Claim 2, wherein said first device implementing the encryption method also comprises a generator for a random integer number r, and wherein said first device:

- performs the drawing of a random integer number r, and

- calculates the cryptogram c by performing the encryption calculation: $c = g^m r^n \bmod (n^2)$.

5. (Amended) A system according to Claim 4, wherein said second device implements a decryption method, in order to decrypt said cryptogram c, which comprises performing the calculation

$m = \log_n(c^{\lambda(n)} \bmod n^2).\log_n(g^{\lambda(n)} \bmod n^2)^{-1} \bmod n$

$$where\ \log_n(x) = \frac{x-1}{n}$$

x being any integer.

6. (Amended) A system according to Claim 5, wherein said second device implementing said decryption method precalculates the quantity:

$\alpha_{n,g} = \log_n(g^{\lambda(n)} \bmod n^2)^{-1} \bmod n$

and stores it secretly in a protected area of a program memory.

7. (Amended) A system according to Claim 5, wherein said second device performs the following calculation steps during said decryption method, using the Chinese Remainder Theorem CRT:

$m_p = \log_p(c^{p-1} \bmod p^2).\log_p(g^{p-1} \bmod p^2)^{-1} \bmod p.$

$m_q = \log_q(c^{q-1} \bmod q^2).\log_q(g^{q-1} \bmod q^2)^{-1} \bmod q.$

$m = CRT(m_p, m_q, p, q)$, where $\log_p$ and $\log_q$ are such that

$$\log_i(x) = \frac{x-1}{i}$$

x being any integer.

8. (Amended) A system according to Claim 7, wherein said second device implementing said decryption method precalculates the following quantities

$\alpha_{p,g} = \log_p(g^{p-1} \bmod p^2)^{-1} \bmod p$ and

$\alpha_{q,g} = \log_q(g^{q-1} \bmod q^2)^{-1} \bmod q$

and stores them secretly in a protected area of a program memory.

9. (Amended) A cryptographic communication system with public and private keys generated according to Claim 1, comprising a communication channel and first and second communicating devices, each device comprising a communication interface, data processing means and storage means, wherein an encryption method is implemented in said first device for sending a number m representing a message, $0 \leq m < n^2$, to said second device, said encryption method comprising the following steps:

- using the parameters of the public key of the second device to assign the values of the public key to the parameters n and g,

- performing the following calculations:

1. $m_1 = m \bmod n$
2. $m_2 = (m-m1)/n$
3. $c = g^{m1} m_2^n \bmod n^2$, and

- transmitting the cryptogram c over the communication channel to the second device.

10. (Amended) A system according to Claim 9, wherein the second device receives the cryptogram c and implements a decryption method, in order to decrypt said cryptogram, which comprises the performance of the following calculation steps:

1. $m_1 = \log_n(c^{\lambda(n)} \bmod n^2).\log_n(g^{\lambda(n)} \bmod n^2)^{-1} \bmod n$
2. $w = cg^{-m1} \bmod n$
3. $m_2 = w^{1/n \bmod \lambda(n)} \bmod n$
4. $m = m_1 + nm_2$.

11. (Amended) A system according to Claim 10, wherein the second device implementing said decryption method precalculates the following quantities:

$\alpha_{n,g} = \log_n(g^{\lambda(n)} \bmod n^2)^{-1} \bmod n$, and

$\gamma_n = 1/n \bmod \lambda(n)$,

and stores them secretly in a protected area of a program memory.

12. (Amended) A system according to Claim 10, wherein said second device performs the following calculation steps during said decryption method, using the Chinese Remainder Theorem:

1. $m_{1,p} = \log_p(c^{p-1} \bmod p^2)\log_p(g^{p-1} \bmod p^2)^{-1} \bmod p$
2. $w_p = cg^{-m1,p} \bmod p$

3. $m_{2,p}=w_p^{1/q \bmod p-1} \bmod p$

4. $m_{1,q}=\log_q(c^{q-1} \bmod q^2).\log_q(g^{q-1} \bmod q^2)^{-1} \bmod q$

5. $w_q=cg^{-m1,q} \bmod q$

6. $m_{2,q}=w_q^{1/p \bmod q-1} \bmod q$

7. $m_1=CRT(m_{1,p},m_{2,p},p,q)$

8. $m_2=CRT(m_{1,q},m_{2,q},p,q)$, and

9. $m = m_1 + pqm_2$ where $\log_p$ and $\log_q$ are such that

$$\log_i(x)=\frac{x-1}{i},$$

and x is any integer.

13. (Amended) A system according to Claim 12, wherein said second device precalculates the following quantities:

$\alpha_{p,g}=\log_p(g^{p-1} \bmod p^2)^{-1} \bmod p$

$\alpha_{q,g}=\log_q(g^{q-1} \bmod q^2)^{-1} \bmod q$

$\gamma_p= 1/q \bmod p-1$

$\gamma_q= 1/p \bmod q-1$

and stores them secretly in a protected memory area of a program memory.

14. (Amended) A system according to claim 10, wherein the decryption method is used for calculating the signature s of a message m and the encryption method is used for verifying said signature.

15. (Amended) A cryptographic communication system with public and private keys generated according to Claim 1, comprising a communication channel and first and second communicating devices, each device comprising a communication interface, data processing means and storage means, wherein an encryption method is implemented in said first device to send a number m representing a message, $0 \leq m < n$, to said second device, said encryption method comprising the following steps:

- using the parameters of the public key of the second device to assign the values of the public key to the parameters n and g,

- calculating the cryptogram $c = g^m \bmod n^2$, and

- transmitting said cryptogram c over the communication channel to the second device.

16. (Amended) A system according to Claim 15, wherein said first device that implements the encryption method also comprises a generator for a random integer number r, and wherein said device:

- performs the drawing of a random integer number r, and

- calculates the cryptogram c, performing the encryption calculation: $c = g^{m+nr} \bmod (n^2)$.

17. (Amended) A system according to Claim 15 wherein the second device implements a method of decryption of the received cryptogram c, comprising the performance of the following calculation:

$m = \log_n(c^u \bmod n^2).\log_n(g^u \bmod n^2)^{-1} \bmod n$,

where u is an integer that divides (p-1) and (q-1).

18. (Amended) A method according to Claim 17, wherein said second device implementing said decryption method precalculates the quantity:

$\beta_{n,g} = \log_n(g^u \bmod n^2)^{-1} \bmod n$

and stores it secretly in a protected area of a program memory.

19. (Amended) A system according to Claim 17, wherein said second device performs the following calculation steps during said decryption method, using the Chinese Remainder Theorem:

1. $m_p = \log_p(c^u \bmod p^2).\log_p(g^u \bmod p^2)^{-1} \bmod p$
2. $m_q = \log_q(c^u \bmod q^2).\log_q(g^u \bmod q^2)^{-1} \bmod q$
3. $m = CRT(m_p, m_q, p, q)$, where $\log_p$ and $\log_q$ are such that

$$\log_i(x) = \frac{x-1}{i}$$

x being any integer.

20. (Amended) A system according to Claim 19, wherein said second device implementing said decryption method precalculates the following quantities:

$\beta_{p,g}=\log_n(g^u \bmod p^2)^{-1} \bmod p$

$\beta_{q,g}=\log_n(g^u \bmod q^2)^{-1} \bmod q$

and stores them secretly in a protected area of a program memory.

REMARKS

Entry of the foregoing amendment is respectfully requested. This amendment is intended to place the claims in a more conventional format and eliminate the multiple dependency of the claims.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

By: _____

James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

Date: July 16, 2001

Attachment to Preliminary Amendment dated July 16, 2001

Marked-up Claims 1-20

1. (Amended) A cryptographic method [comprising a method of] for generating public [(K)] and private [(K')] keys in a device that is able to exchange messages on at least one communication channel, the private key [having to be] being stored secretly in [the] said device and the public key [having to be] being broadcast publicly, the generation method comprising the following steps:

- selecting two prime numbers p and q which are distinct and of [adjacent] similar sizes;

- calculating the number n equal to the product of p and q [p,q];

- calculating the lowest common multiple of the numbers (p-1) and (q-1): $\lambda(n)=LCM(p-1, q-1)$

- determining a number g, $0 \leq g < n^2$, which satisfies the following two conditions during the calculation of a cryptogram c[:] , where $c=g^m \bmod n^2$:

a) g is invertible modulo n^2, and

b) $ord(g,n^2) = 0 \bmod n$, and

- selecting g = 2 if g satisfies said conditions a) and b);

wherein the public key of [the] said device [being] is formed by the parameters n and g and its private key [being] is formed by [the parameters p,q and $\lambda(n)$ or by the] at least the parameters p and q[, a generation method characterised in that it consists in taking g=2, if g satisfies the said conditions a) and b)].

Attachment to Preliminary Amendment dated July 16, 2001

Marked-up Claims 1-20

2. (Amended) A cryptographic communication system with public and private keys generated according to Claim 1, comprising a communication channel [(20)] and first and second communicating devices [(A, B)], each device comprising at least one communication interface [(11)], data processing means [(10)] and storage means [(12, 13), characterised in that], wherein an encryption method is implemented in [a] said first device [(A) in order] to send a number m representing a message, $0 \leq m < n$, to [a] said second device [(B), the], said encryption method comprising the following steps:

- using the parameters of the public key [(n_B, g_B)] of the second device [(B) in order] to assign the values of the public key [(n_B, g_B)] to the parameters n and g,

- calculating the cryptogram $c = g^m \bmod n^2$, and

- transmitting [the] said cryptogram [c then being transmitted] over the communication channel to the second device.

3. (Amended) A system according to Claim 2, [characterised in that the] wherein said first device implementing the encryption method also comprises a generator [(15)] for a random integer number r, and [in that the said] wherein said first device:

- performs the drawing of a random integer number r, and [then]

- calculates the cryptogram c by performing the [following] encryption calculation: $c = g^{m+nr} \bmod (n^2)$.

Attachment to Preliminary Amendment dated July 16, 2001

Marked-up Claims 1-20

4. (Amended) A system according to Claim 2, [characterised in that the] wherein said first device implementing the encryption method also comprises a generator [(15)] for a random integer number r, and [in that the said] wherein said first device:

- performs the drawing of a random integer number r, and [then]

- calculates the cryptogram c by performing the [following] encryption calculation: $c=g^m r^n \bmod(n^2)$.

5. (Amended) A system according to Claim 4, [characterised in that the] wherein said second device [(B)] implements a decryption method, in order to decrypt [the] said cryptogram c, [and] which comprises [the] performing [of] the calculation

$$m= \log_n(c^{\lambda(n)} \bmod n^2).\log_n(g^{\lambda(n)} \bmod n^2)^{-1} \bmod n$$

$$\textit{where } \log_n(x)=\frac{x-1}{n}.$$

x being any integer

6. (Amended) A system according to Claim 5, [characterised in that a device (B)] wherein said second device implementing [the] said decryption method precalculates the quantity:

$$\alpha_{n,g}=\log_n(g^{\lambda(n)} \bmod n^2)^{-1} \bmod n$$

Attachment to Preliminary Amendment dated July 16, 2001

Marked-up Claims 1-20

and stores it secretly in [the] a protected area of [the] a program memory[, x being any integer].

7. (Amended) A system according to Claim 5, [characterised in that, in one instance of the said decryption method, a] wherein said second device performs the following calculation steps during said decryption method, using the Chinese Remainder Theorem CRT:

$m_p = \log_p(c^{p-1} \bmod p^2).\log_p(g^{p-1} \bmod p^2)^{-1} \bmod p$.

$m_q = \log_q(c^{q-1} \bmod q^2).\log_q(g^{q-1} \bmod q^2)^{-1} \bmod q$.

$m = CRT(m_p, m_q, p, q)$, where $\log_p$ and $\log_q$ are such that

$$\log_i(x) = \frac{x-1}{i}$$

x being any integer.

8. (Amended) A system according to Claim 7, [characterised in that a] wherein said second device implementing [the] said decryption method precalculates the following quantities

$\alpha_{p,g} = \log_p(g^{p-1} \bmod p^2)^{-1} \bmod p$ and

$\alpha_{q,g} = \log_q(g^{q-1} \bmod q^2)^{-1} \bmod q$

Attachment to Preliminary Amendment dated July 16, 2001

Marked-up Claims 1-20

and stores them secretly in [the] a protected area of [the] a program memory.

9. (Amended) A cryptographic communication system with public and private keys generated according to Claim 1, comprising a communication channel [(20)] and first and second communicating devices [(A,B)], each device comprising a communication interface [(11)], data processing means [(10)] and storage means [(12, 13), characterised in that], wherein an encryption method is implemented in [a] said first device [(A)] for sending a number m representing a message, $0 \leq m < n^2$, to [a] said second device [(B), the] said encryption method comprising the following steps:

- using the parameters of the public key $[K_B=(n_B,g_B)]$ of the second device [(B) in order] to assign the values of the public key $[(n_B,g_B)]$ to the parameters n and g,

- [and] performing the following calculations:

1. $m_1 = m \bmod n$
2. $m_2 = (m-m1)/n$
3. $c = g^{m1} m_2^n \bmod n^2$

[the said] transmitting the cryptogram c [being transmitted] over the communication channel to the second device.

10. (Amended) A system according to Claim 9, [characterised in that] wherein the second device [(B)] receives the cryptogram c and implements a decryption method, in

Attachment to Preliminary Amendment dated July 16, 2001

Marked-up Claims 1-20

order to decrypt [the] said cryptogram, which comprises the performance of the following calculation steps:

1. $m_1 = \log_n(c^{\lambda(n)} \bmod n^2).\log_n(g^{\lambda(n)} \bmod n^2)^{-1} \bmod n$
2. $w = cg^{-m1} \bmod n$
3. $m_2 = w^{1/n \bmod \lambda(n)} \bmod n$
4. $m = m_1 + nm_2$.

11. (Amended) A system according to Claim 10, [characterised in that a] wherein the second device implementing [the] said decryption method precalculates the following quantities:

$\alpha_{n,g} = \log_n(g^{\lambda(n)} \bmod n^2)^{-1} \bmod n$, and

$\gamma_n = 1/n \bmod \lambda(n)$,

and stores them secretly in [the] a protected area of [the] a program memory.

12. (Amended) A system according to Claim 10, [characterised in that, in one instance of the said decryption method, a] wherein said second device performs the following calculation steps during said decryption method, using the Chinese Remainder Theorem:

1. $m_{1,p} = \log_p(c^{p-1} \bmod p^2)\log_p(g^{p-1} \bmod p^2)^{-1} \bmod p$
2. $w_p = cg^{-m1,p} \bmod p$

Attachment to Preliminary Amendment dated July 16, 2001

Marked-up Claims 1-20

3. $m_{2,p}=w_p^{1/q \bmod p-1} \bmod p$

4. $m_{1,q}=\log_q(c^{q-1} \bmod q^2).\log_q(g^{q-1} \bmod q^2)^{-1} \bmod q$

5. $w_q=cg^{-m1,q} \bmod q$

6. $m_{2,q}=w_q^{1/p \bmod q-1} \bmod q$

7. $m_1=CRT(m_{1,p},m_{2,p},p,q)$

8. $m_2=CRT(m_{1,q},m_{2,q},p,q)$, and

9. $m = m_1 + pqm_2$ where $\log_p$ and $\log_q$ are such that

$$\log_i(x)=\frac{x-1}{i},$$

and x is any integer.

13. (Amended) A system according to Claim 12, [characterised in that, in one instance of the said decryption method, a] wherein said second device precalculates the following quantities:

$\alpha_{p,g}=\log_p(g^{p-1} \bmod p^2)^{-1} \bmod p$

$\alpha_{q,g}=\log_q(g^{q-1} \bmod q^2)^{-1} \bmod q$

$\gamma_p= 1/q \bmod p-1$

$\gamma_q= 1/p \bmod q-1$

Attachment to Preliminary Amendment dated July 16, 2001

Marked-up Claims 1-20

and stores them secretly in [the] a protected memory area of [the] a program memory.

14. (Amended) A system according to [any one of Claims 10 to 13, in which] claim 10, wherein the decryption method is used for calculating the signature s of a message m and the encryption method is used for verifying [the] said signature.

15. (Amended) A cryptographic communication system with public and private keys generated according to Claim 1, comprising a communication channel [(20)] and first and second communicating devices [(A, B)], each device comprising a communication interface [(11)], data processing means [(10)] and storage means [(12, 13), characterised in that], wherein an encryption method is implemented in [a] said first device [(A) in order] to send a number m representing a message, $0 \leq m < n$, to [a] said second device [(B), the], said encryption method comprising the following steps:

- using the parameters of the public key $[(n,g)_B]$ of the second device [(B) in order] to assign the values of the public key $[(n_B,g_B)]$ to the parameters n and g,

- calculating the cryptogram $c = g^m \bmod n^2$, and

[the] transmitting said cryptogram c [then being transmitted] over the communication channel to the second device.

Attachment to Preliminary Amendment dated July 16, 2001

Marked-up Claims 1-20

16. (Amended) A system according to Claim 15, [characterised in that the] wherein said first device that implements the encryption method also [comprising] comprises a generator [(15)] for a random integer number r, and [in that the] wherein said device:

- performs the drawing of a random integer number r, and [then]

- calculates the cryptogram c, performing the [following] encryption calculation:

$c = g^{m+nr} \bmod (n^2)$.

17. (Amended) A system according to Claim 15 [or 16, characterised in that] wherein the second device implements a method of decryption of the received cryptogram c, comprising the performance of the following calculation:

$m = \log_n(c^u \bmod n^2).\log_n(g^u \bmod n^2)^{-1} \bmod n$,

where u is an integer that divides (p-1) and (q-1).

18. (Amended) A method according to Claim 17, [characterised in that a] wherein said second device implementing [the] said decryption method precalculates the quantity:

$\beta_{n,g} = \log_n(g^u \bmod n^2)^{-1} \bmod n$

and stores it secretly in [the] a protected area of [the] a program memory.

Attachment to Preliminary Amendment dated July 16, 2001

Marked-up Claims 1-20

19. (Amended) A system according to Claim 17, [characterised in that, in one instance of the said decryption method, a] wherein said second device performs the following calculation steps during said decryption method, using the Chinese Remainder Theorem:

1. $m_p = \log_p(c^u \bmod p^2).\log_p(g^u \bmod p^2)^{-1} \bmod p$
2. $m_q = \log_q(c^u \bmod q^2).\log_q(g^u \bmod q^2)^{-1} \bmod q$
3. $m = CRT(m_p, m_q, p, q)$, where $\log_p$ and $\log_q$ are such that

$$\log_i(x) = \frac{x-1}{i}$$

x being any integer.

20. (Amended) A system according to Claim 19, [characterised in that a] wherein said second device implementing [the] said decryption method precalculates the following quantities:

$\beta_{p,g} = \log_n(g^u \bmod p^2)^{-1} \bmod p$

$\beta_{q,g} = \log_n(g^u \bmod q^2)^{-1} \bmod q$

and stores them secretly in [the] a protected area of [the] a program memory.

ART 34 AMDT

4/PR75

09/889362

JC18 Rec'd PCT/PTO 16 JUL 2001

PUBLIC AND PRIVATE KEY CRYPTOGRAPHIC METHOD

The present invention relates to a public and private key cryptographic method. It can be used in all applications in which it is necessary to ensure confidentiality of the messages transmitted over any channel and/or to identify with certitude a device with which messages have been exchanged.

The confidentiality of messages transmitted between two devices A and B over any communication channel is obtained by encryption of the information transmitted in order to make it unintelligible to any persons for whom it is not intended. The sure identification of a message is for its part based on the calculation of the digital signature of a message.

In practice, two types of cryptographic method can be used, the so-called symmetrical one, with secret keys, a well-known example of which is the DES… the so-called asymmetric one, using a pair of public and private keys and described in "Public-key cryptosystem" in "New Directions in Cryptography", IEEE Transactions

on Information Theory, Nov. 1976, by Messrs Diffie and Hellman. A well-known example of an asymmetric method is the RSA, from the name of its inventors Ronald Rivest, Adi Shamir and Leonard Adleman. A description of this RSA method can be found in US patent 4.405.829.

In the invention, the concern is more particularly with an asymmetric cryptographic method.

An encryption method according to an asymmetric cryptographic method consists mainly, for a transmitter A which wishes to confidentially send a message to a destination B, in taking cognisance, for example in a directory, of the public key K_B of the destination B, applying in the encryption method E to the message m to be transmitted, using this public key, and sending, to the destination B, the resulting cryptogram :

c: $c=E_{KB}(m)$.

This method consists mainly, for the destination B, in receiving the cryptogram c, and decrypting it in order to obtain the original message m, applying the private key K'b which it alone knows in the decryption method D to the cryptogram c: m=Dk'b(c).

According to this method anyone can send an encrypted message to the destination B, but only the latter is capable of decrypting it.

Normally an asymmetric cryptographic method is used for the generation/verification of the signature. In this context, a user who wishes to prove his identity uses a private key, known to him alone, to produce a digital signature s of a message m, a signature which he transmits to the destination device.

The latter implements the verification of the signature using the public key of the user. Any device thus has the capability of verifying the signature of a user, taking cognisance of the public key of this user and applying it in the verification algorithm. However, only the user concerned has the ability to generate the correct signature using his private key. This method is for example much used in access control systems or banking transactions. It is in general coupled with the use of an encryption method, for encryption of the signature before transmitting it.

For this generation/verification of digital signatures, it is possible to use in practice asymmetric cryptographic methods dedicated to this application, such as the DSA (Digital Signature Algorithm), which corresponds to an American standard proposed by the US National Institute of Standards and Technology. It is also possible to use the RSA, which has the property of being able to be used both in encryption and in signature generation.

In the invention, the concern is with a cryptographic method which can be used for the encryption of messages and for the generation of a digital signature. In the current state of the art, only the RSA, of which there exist many variant implementations, offers this double functionality.

The RSA comprises a step of generating the public K and private K' keys for a given device in which the procedure is as follows:

- two distinct large prime numbers p and q are chosen,

- their product n=p.q is calculated,

- a prime number is chosen with the lowest common multiple of (p-1)(q-1). In practice, e is often taken to be equal to 3.

The public key K is then formed by the pair of parameters (n,e) and the secret key K' is formed by the pair of parameters (p,q).

By choosing p and q of large size, their product n is also of large size. n is therefore very difficult to factorise: it is ensured that it will not be possible to find the secret key K'=(p,q) from a knowledge of n.

The method of encryption of a number m representing a message M, $0 \leq m < n$ then consists in performing the following calculation:

$c = E_B(m) = m^e \bmod n$

by means of the public key K=(n,e).

The decryption method then for its part consists of the following reverse calculation:

$m = c^d \bmod (n)$

by means of the private key K'=(p,q), kept secret, where

$$d = \frac{1}{e} \bmod (p-1)(q-1).$$

It has been seen that the RSA has the particularity of being able to be used for signature verification. The corresponding method of signature generation by a user A consists in using the decryption

method with the secret key in order to produce the signature s of a number m representing a message. Thus: $s=m^d \bmod n$.

This signature s is transmitted to a destination B. The latter, who knows m (for example, A transmits s and m), verifies the signature by performing the reverse operation, that is to say using the encryption method with the public key of the transmitter A. That is to say he calculates $v=s^e \bmod n$, and verifies v=m.

In general, to improve the security of such a signature verification method, a hash function is first applied to the number m before calculating the signature, which can consist of permutations of bits and/or a compression.

When a message M to be encrypted or signed is spoken of, it is a case of course of digital messages, which can result from prior digital coding. These are in practice strings of bits, whose binary size (the number of bits) can be variable.

However, a cryptography method such as the RSA is such that it makes it possible to encrypt, with the public key (n,e), any number between 0 and n-1. In order to apply it to a message M of any size, it is therefore necessary in practice to divide this message into a series of numbers m which will each satisfy the condition $0 \leq m < n$. Then the encryption method is applied to each of these numbers. Hereinafter, the concern is therefore with the application of the cryptographic method to a number m representing the message M. m can be equal to M, or be only a part thereof. Hereinafter

m is used indifferently to designate the message or a number representing the message.

One object of the invention is an asymmetric cryptography method different from those based on the RSA.

One object of the invention is a method based on other properties, which can be applied either to the encryption of messages or to the generation of signatures.

One object of the invention is a cryptography method which affords, in certain configurations, a more rapid processing time.

As characterised, the invention relates to a cryptography method according to Claim 1.

The invention will be better understood from a reading of the following description, given as an indication and in no way limitative of the invention, and with reference to the accompanying drawings, in which:

- Figure 1 is a functional diagram of a cryptographic communication system of the asymmetric type;

- Figure 2 is a functional diagram of a communicating device used in a cryptographic communication system according to the invention;

- Figure 3 is a flow diagram of a message encryption/decryption session using the cryptographic method according to the invention; and

- Figure 4 is a flow diagram of a signature generation/verification session using the cryptographic method according to the invention.

In order to clearly understand the invention, it is necessary to carry out a few mathematical preliminaries.

In the description, the following mathematical notations are used:

(1) If a is a relative integer and b a strictly positive integer, a mod b (a modulo b) is the modular residue of a relatively to b and designates the unique integer strictly less than b such that b divides (a - a mod b).

(2) (Z/bZ) designates the set of residues modulo b and forms a group for the modular addition.

(3) (Z/bZ)* designates the set of integers invertible modulo b and forms a group for the modular multiplication.

(4) The order of an element a of (Z/bZ)* is the smallest natural integer ord(a,b) such that $a^{ord(a,b)}=1$ mod b.

(5) LCM(a,b) designates the lowest common multiple of a and b.

(6) HCF(a,b) designates the highest common factor of a and b.

(7) $\lambda(a)$ designates the Euler indicator of a. If a=p.q, $\lambda(a)$=LCM(p-1, q-1).

(8) The unique solution, obtained by using the well-known Chinese Remainder Theorem, of the following system of modular equations:

$x=a_1 \bmod b_1$

$x=a_2 \bmod b_2$

...

$x=a_k \bmod b_k$

where the integers a_i and b_i are given and where $\forall i,j$ with $i \neq j$, $HCF(bi,bj)=1$, is denoted $x=CRT(a_1,...a_k, b_1,...b_k)$.

(9) The binary size of a number a is the number of bits in which a is written.

Now let n be an integer number of arbitrary size. The set $Un=\{x<n^2 / x=1 \bmod n\}$ is a multiplicative subgroup of $(Z/n^2Z)^*$.

Then let $\log_n$ be the function defined on the set Un by:

$$\log_n(x)=\frac{x-1}{n}$$

This function has the following property:

$\forall\ x \in Un$, $\forall\ y \in Un$, $\log_n(xy \bmod n^2)= \log_n(x) + \log_n(y) \bmod n$.

Consequently, if g is an arbitrary integer number belonging to Un, this gives, for any number m, $0 \leq m < n$:

$\log_n(g^m \bmod n^2)=m.\log_n(g) \bmod n$.

This mathematical property is at the basis of the cryptography method used in the invention, which will now be described.

Figure 1 shows a cryptographic communication system, using an asymmetric cryptographic method. It comprises devices communicating, in examples A and B, on a communication channel 1. The example shows a

bidirectional channel. Each device contains a pair of public K and private K' keys.

The public keys are for example published in a public file 2 such as a directory, which each device can consult. In this public file, there will thus be found the public key K_A of the device A and the public key K_B of the device B.

The private key K' of each device is stored by it secretly, typically in a protected non-volatile memory area. The device A thus contains in secret memory its private key K'_A and the device B thus contains in secret memory its private key K'_B. They also store their public key, but in a memory area without any particular access protection.

In such a system, the device A can encrypt a message m in a cryptogram c_A using the public key K_B of the device B; the latter can decrypt c_A using its private key K'_B, which it stores secretly. Conversely, the device B can encrypt a message m in a cryptogram c_B using the public K_A of the device A. The latter can decrypt c_B using its private key K'_A, which it stores secretly.

Typically, each device comprises at least, as shown in Figure 2, processing means 10, that is to say a central processing unit (CPU), comprising notably different registers R for the calculation, an interface 11 for communication with the communication channel, and storage means. These storage means generally comprise a program memory 12 (ROM, EPROM, EEPROM) and a working memory (RAM) 13. In practice, each device

stores its secret data in a protected access area 120 provided in the program memory and its public data in a normal access area of this memory. The working memory makes it possible to store temporarily, for the time required for the calculations, messages to be encrypted, cryptograms to be decrypted, or intermediate calculation results.

The processing and storage means thus make it possible to execute programs related to the application, and notably to make the calculations corresponding to the implementation of the cryptography method for the encrypting/decrypting of messages and/or the generation/verification of signatures according to the invention. These calculations comprise notably, as will be seen in detail hereinafter, raisings to the power, residues, and modular inversions.

The devices can also comprise a generator 14 for a random or pseudo-random number r, which can participate in the aforementioned calculations, in certain variant embodiments. This generator is framed in dotted lines in Figure 2, in order to indicate that it is not necessary for the implementation of all the variant embodiments according to the invention.

All these means of the device are connected to an address and data bus 15.

Such devices used in the invention are well known, and correspond for example to those which are used in the cryptographic communication systems of the state of the art, using the RSA. They will therefore not be detailed any further. One practical example of a

cryptographic communication system is the system formed by banking servers and smart cards, for managing financial transactions. However, there are many other applications, such as the applications related to electronic commerce.

A first embodiment of the invention will now be detailed, with regard to the flow diagram shown in Figure 3.

This flow diagram shows a communication sequence between a device A and a device B on a communication channel 20. These devices comprise at least the processing, storage and communication means described in relation to Figure 2.

The cryptography method according to the invention comprises a method of generating public K and private K' keys.

According to the invention, this method of generating public and private keys of a device comprises the following steps, which are already known in the document of Yasuko Gotoh et al, published in January 1990 in Japan, under the references XP000177817, ISSN: 0882-1666, Vol 21, N° 8, pages 11-20, of "a method for rapid RSA key generation" from the work "Systems and Computers":

- selection of two large prime numbers p and q which are distinct and of adjacent sizes;
- calculation of the number n equal to the product p.q;

- calculation of the number $\lambda(n)=LCM(p-1, q-1)$, that is to say of the Carmichael function of the number n;

- determination of a number g, $0 \leq g < n^2$, which fulfils the following two conditions:

a) g is invertible modulo n^2, and

b) $ord(g,n^2)=0 \bmod n$.

This condition b) indicates that the order of the number g in the set $(Z/n^2Z)^*$ of the integer numbers from 0 to n^2 is a non-zero multiple of the number n, according to the notations defined above.

The public key K is then formed by the number n and the number g. The private key is formed by the numbers p,q and $\lambda(n)$ or only by the numbers p and q, $\lambda(n)$ being able to be recalculated at each use of the secret key.

The public and private keys of each device are generated according to this method. This generation can be effected, according to the devices considered and the applications, by the devices themselves or by an external component.

Each device, for example the device A, therefore contains in memory its public key $K_A = (n_A, g_A)$ and, secretly, its private key $K'_A=(p_A, q_A)$.

In addition, the public keys are put in a file accessible to the public.

According to the invention, it will be seen below that it consists in giving a particular value to g. This is because it is advantageous to choose g=2, when

possible, that is to say when g=2 fulfils conditions a) and b) of the signature generation method according to the invention.

An encryption method according to a first embodiment of the cryptographic method of the invention implemented in the device A then consists, for sending a message to the device B, of the performance of the following steps, with $0 \leq m < n$:

- giving information on the parameters n and g of the encryption method implemented by the device A by means of the public key K_B of the second device B: $n = n_B$, $g = g_B$,
- calculating the cryptogram $c = g^m \bmod n^2$, and
- transmitting the cryptogram c over the communication channel.

The encryption method according to a first embodiment of the invention therefore consists in taking the parameter g of the public key, raising it to the power m, and calculating the modular residue relatively to n^2. It should be noted that, in the RSA, it is the message m which is raised to the power whilst in the invention the message m is used as an exponent.

The device B which receives the encrypted message, that is to say the cryptogram c, then implements a decryption method according to the invention with the parameters of its private key. This decryption method comprises the following calculation:

- calculation of the number m such that

$$m = \frac{\log_n(c^{\lambda(n)} \bmod n^2)}{\log_n(g^{\lambda(n)} \bmod n^2)} \bmod n$$

where

$$\log_n(x)\frac{x-1}{n}.$$

If g=2, it can be seen that the calculation of raising g to the power is facilitated. Therefore preferably g=2 will be taken, whenever possible. In other words, the method of generating the keys will commence by seeing whether g=2 fulfils conditions a) and b).

Different variants of the calculation of the decryption method can be implemented, which make it possible, when the device must decrypt a large number of cryptograms, to precalculate certain quantities and to store them secretly in the device. One corollary is that the secret memory area (area 120 in Figure 2) of the device must be more extensive, since it must then contain additional parameters in addition to the parameters p and q. This is not without influence on the choice of implementing one variant or another. This is because the implementation of a protected memory area is expensive, and therefore with a generally limited (memory) capacity, notably in the so-called low-cost devices (for example certain types of smart card).

In a first variant embodiment of the decryption device, provision is made for the device, B in this case, to precalculate once and for all the quantity:

$$\alpha_{n,g}= \log_n(g^{\lambda(n)} \bmod n^2)^{-1} \bmod n$$

and to keep it secret in memory.

Thus the time necessary for the decryption of each of the messages received by the device is reduced accordingly. This is because, when the device B executes an instance of this variant of the decryption method, all that is left for it to do is to calculate:

$m = \log_n(c^{\lambda(n)} \bmod n^2)\ \alpha_{n,g} \bmod n$.

In a second variant embodiment of the decryption method according to the invention, provision is made for using the Chinese Remainder Theorem, for better efficiency (speed of calculation).

In one instance of this second variant of the decryption method, the device performs the following (decryption) calculations:

1 $m_p = \log_p(c^{p-1} \bmod p^2) \log_p(g^{p-1} \bmod p^2)^{-1} \bmod p$

2 $m_q = \log_q(c^{q-1} \bmod q^2) \log_p(g^{q-1} \bmod q^2)^{-1} \bmod q$

3 $m = CRT(m_p, m_q, p, q)$,

where

$$\log_p(x) \frac{x-1}{p} \text{ and}$$

$$\log_q(x) \frac{x-1}{q}$$

In this case, provision can also be made, in the cases where the device has to decrypt a very large number of messages, for the device to precalculate once and for all the following quantities:

$\alpha_{p,g} = \log_p(g^{p-1} \bmod p^2)^{-1} \bmod p$ and

$\alpha_{q,g} = \log_q(g^{q-1} \bmod q^2)^{-1} \bmod q$.

The device must then store these quantities as secret data.

The calculation made during one instance of the decryption method becomes:

1. $m_p = \log_p(c^{p-1} \bmod p^2)\ \alpha_{p,g} \bmod p$
2. $m_q = \log_q(c^{q-1} \bmod q^2)\ \alpha_{q,g} \bmod q$
3. $m = CRT(m_p, m_q, p, q)$.

As already stated, all its variant decryption calculations are advantageous when the device has to decrypt a very large number of messages, and when the saving in processing time compensates for the larger memory capacity of the protected area for storing all the secret data. The choice of one or other variant depends in practice on the application in question and the constraints of cost and processing time to be reconciled.

A second embodiment of the invention comprises the use of a random number, supplied by a random (or pseudo-random) number generator, in the encryption method, so that, for the same message m to be transmitted, the calculated cryptogram c will be different on each occasion. The security of the communication system is therefore greater. The decryption method is unchanged.

This second embodiment of the invention comprises two variants.

In a first variant, the cryptogram c is obtained by the following calculation: $c = g^{m+nr} \bmod n^2$.

In a second variant, the cryptogram c is obtained by the following calculation: $c = g^m r^n \bmod n^2$.

This second variant requires in practice a longer processing time than the first, but offers greater security.

In a third embodiment of the invention, the condition is imposed that the order of g in $(Z/nZ)^*$ be a small integer, this being obtained by the implementation of a different key generation method.

With such a condition on the order of the parameter g, the complexity of the calculation of the decryption method, which in practice becomes quadratic (a function of n^2) with respect to the size of the number n, is reduced.

In this third embodiment of the invention, the method of generating the public and private keys is then as follows:

- selecting in secret an integer u and two large prime numbers p and q which are distinct and of adjacent sizes, such that u divides (p-1) and divides (q-1);
- calculating the number n equal to the product p.q;
- calculating the number $\lambda(n)=LCM(p-1, q-1)$, that is to say of the Carmichael indicator of the number n;
- determining a number h, $0 \leq h < n^2$, which fulfils the following two conditions:
  a) h is invertible modulo n^2, and
  b) $ord(h,n^2)=0 \bmod n$.
- calculating the number $g = h^{\lambda(n)/u} \bmod n^2$.

The public key K is then formed by the number n and the number g. The private key consists of the integers (p,q,u) stored secretly in the device.

Preferably h=2 is chosen, when possible (that is to say if h=2 fulfils conditions a) and b), in order to facilitate the calculation of g).

It should be noted that, if u = HCF(p-1,q-1), it is not necessary to store this number, which can be found by the device from p and q.

Preferably u will be chosen prime, in order to improve the security of the method, and of small size, typically 160 bits. By choosing a small size for u, it will be seen that the decryption calculation is facilitated.

In this third embodiment, the implementation of the encryption method to encrypt a message m is identical to the one previously described in the first embodiment of the invention, the cryptogram being equal to $c=g^m \bmod n^2$.

It is also possible to calculate the cryptogram c by using a random variable r according to the first variant of the second embodiment of the invention previously described. r is then a random integer, with the same size as u, and the cryptogram is obtained by the following calculation: $c=g^{m+nr} \bmod n^2$.

The cryptogram c calculated according to one or other previous implementation of the encryption method is sent to the device B, which must decrypt it. The implementation of the decryption method by the device B which receives the message is a little different.

This is because the calculation made in the device in one instance of decryption, in order to find the number m from the cryptogram c, becomes the following:

$$m = \frac{\log_n(c^u \bmod n^2)}{\log_n(g^u \bmod n^2)} \bmod n .$$

As before, it is possible to apply variant calculations, which make it possible to accelerate the processing time needed.

In a first variant, the quantity:

$$\beta_{n,g} = \log_n(g^u \bmod n^2)^{-1} \bmod n$$

will thus be precalculated once and for all and will be stored secretly in memory.

During one instance of decryption of a cryptogram c received, the device then merely has to make the following calculation:

$$m = \log_n(c^u \bmod n^2)\ \beta_{n,g} \bmod n.$$

In a second variant, the Chinese Remainder Theorem is implemented, using the functions $\log_p$ and $\log_q$, already seen for performing the decryption calculation.

During one instance of this variant of the method of decrypting the cryptogram c received, the device then performs the following calculations:

1. $m_p = \log_p(c^u \bmod p^2)\log_p(g^u \bmod p^2)^{-1} \bmod p$
2. $m_q = \log_q(c^u \bmod q^2)\log_q(g^u \bmod q^2)^{-1} \bmod q$
3. $m = CRT(m_p, m_q, p, q)$.

In a third variant, the processing time needed for the decryption of the cryptogram c according to the second variant is accelerated still further, precalculating the following quantities:

$$\beta_{p,g} = \log_p(g^u \bmod p^2)^{-1} \bmod p$$

$\beta_{q,g} = \log_q(g^u \bmod q^2)^{-1} \bmod q$

and storing them secretly in the device.

During an instance of calculation of this third variant of the method of decrypting the cryptogram c received, the device then merely has to perform the following calculations:

1. $m_p = \log_p(c^u \bmod p^2)\ \beta_{p,g} \bmod p$
2. $m_q = \log_q(c^u \bmod q^2)\ \beta_{q,g} \bmod q$
3. $m = CRT(m_p, m_q, p, q)$.

In a fourth embodiment of the invention, the encryption method and the decryption method are such that they have the particularity of being permutations on the group of integers modulo n^2. In other words, if the message m is expressed in k bits, the cryptogram c obtained by applying the encryption method to m and the signature s obtained by applying the decryption method to m are also in k bits.

This particularity confers on the cryptographic method the additional property of being able to be used both for encryption/decryption and for signature generation/verification. In this case, the decryption method is employed as a signature generation method and the encryption method as a signature verification method.

In this fourth embodiment, the method of generating public and private keys is the same as that of the first embodiment of the invention: $K=(n,g)$ and $K'=(p,q,\lambda(n))$ or $K'=(p,q)$.

If the device A wishes to send an encrypted message m to the device B, it obtains the public key (n,g) from the latter, and then, in one instance of the encryption method, then performs the following calculations, applied to the number m, $0 \leq m < n^2$:

1. $m_1 = m \bmod n$
2. $m_2 = (m - m1)/n$ (Euclidian division)
3. $c = g^{m1}\, m_2^{\,n} \bmod n^2$.

It is this cryptogram c which is sent to the device B.

The latter must therefore apply the corresponding decryption method to it, in order to find m_1, m_2 and finally m. This decryption method according to the fourth embodiment of the invention consists in performing the following calculations:

1. $m_1 = \log_n(c^{\lambda(n)} \bmod n^2).\log_n(g^{\lambda(n)} \bmod n^2)^{-1} \bmod n$.
2. $w = cg^{-m1} \bmod n$.
3. $m_2 = w^{1/n \bmod \lambda(n)} \bmod n$.
4. $m = m_1 + nm_2$.

As before, variants of the decryption method according to this fourth embodiment of the invention are applicable, which make it possible to reduce the processing time necessary for decrypting a given message. They are advantageous when the device has a large number of cryptograms to decrypt.

A first variant consists in precalculating the following quantities:

$\alpha_{n,g} = \log_n(g^{\lambda(n)} \bmod n^2)^{-1} \bmod n$ and

$\gamma_n = 1/n \bmod \lambda(n)$

which the device B calculates once and for all and keeps secret in memory.

At each new instance of decryption of a cryptogram c received according to this first variant, the device B merely has to perform the following calculations:

1. $m_1=\log_n(c^{\lambda(n)} \bmod n^2)\ \alpha_{n,g} \bmod n$.
2. $w=cg^{-m1} \bmod n$.
3. $m_2=w^m \bmod n$.
4. $m = m_1 + nm_2$.

In a second variant of the implementation of the decryption method according to the fourth embodiment, the Chinese Remainder Theorem is used.

The device which wishes to decrypt a cryptogram c according to this second variant then performs the following successive calculations:

1. $m_{1,p}=\log_p(c^{p-1} \bmod p^2)\log_p(g^{p-1} \bmod p^2)^{-1} \bmod p$
2. $w_p=cg^{-m1,p} \bmod p$
3. $m_{2,p}=w_p^{1/q \bmod p-1} \bmod p$
4. $m_{1,q}=\log_q(c^{q-1} \bmod q^2)\log_q(g^{q-1} \bmod q^2)^{-1} \bmod q$
5. $w_q=cg^{-m1,q} \bmod q$
6. $m_{2,q}=w_q^{1/p \bmod q-1} \bmod q$
7. $m_1=CRT(m_{1,p},m_{2,p},p,q)$.
8. $m_2=CRT(m_{1,q},m_{2,q},p,q)$.
9. $m = m_1 + pqm_2$.

In a third variant, in order to further improve the time for processing the decryption of this second variant, the device B can precalculate once and for all the following quantities:

$\alpha_{p,g}=\log_p(g^{p-1} \bmod p^2)^{-1} \bmod p$

$\alpha_{q,g}=\log_q(g^{q-1} \bmod q^2)^{-1} \bmod q$

$\gamma_p = 1/q \bmod p-1$

$\gamma_q = 1/p \bmod q-1$

and keep them secret in memory.

The device which wishes to decrypt a cryptogram c according to this third variant merely has to perform the following calculations:

1. $m_{1,p} = \log_p(c^{p-1} \bmod p^2)\ \alpha_{p,q} \bmod p$
2. $w_p = cg^{-m1,p} \bmod p$
3. $m_{2,p} = w_p^{\gamma p} \bmod p$
4. $m_{1,q} = \log_q(c^{q-1} \bmod q^2)\ \alpha_{q,q} \bmod q$
5. $w_q = cg^{-m1,q} \bmod q$
6. $m_{2,q} = w_q^{\gamma q} \bmod q$
7. $m_1 = CRT(m_{1,p}, m_{2,p}, p, q)$.
8. $m_2 = CRT(m_{1,q}, m_{2,q}, p, q)$.
9. $m = m_1 + pqm_2$.

The fourth embodiment of the invention which has just been described makes it possible to carry out the signature generation/verification. As shown in the flow diagram in Figure 4, if the device B has to generate a signature s of a number m representing a message to the device A, it applies, as a signature generation method, the decryption method with its private key: $s = D_{K',B}(m)$.

The device A, which receives the signature s and which knows the message m, checks that the signature is correct by calculating the quantity v obtained by applying the encryption method to the signature s with the public key: $v = E_{KB}(s)$. If the signature is correct, $v = m$.

All the variant embodiments of the decryption method of this fourth embodiment which make it possible to accelerate the processing time are also clearly applicable in signature generation/verification.

The invention which has just been described is applicable in all the systems in which it is wished to be able to encrypt and/or sign messages. It broadens the possibilities of adaptation to different applications, depending on whether more security is sought, or increased processing speed. In this regard, it should be noted that the third embodiment of the invention, whose calculation complexity is only quadratic (function of n^2) offers a real advantage in terms of speed, in so far as all the methods of the state of the art have a higher order of complexity (function of n^3). Such an advantage more particularly relates to all the applications using portable devices, such as smart cards and more particularly low-cost devices.

Finally, any person experienced in the art to which the invention relates will understand that modifications to the form and/or details can be made. In particular the signature can be encrypted, or a hash function can be applied to the message m before calculating its signature. This makes it possible to have notably a different signature each time even if the message m is unchanged.

CLAIMS

1. A cryptographic method comprising a method of generating public (K) and private (K') keys in a device able to exchange messages on at least one communication channel, the private key having to be stored secretly in the said device and the public key having to be broadcast publicly, the generation method comprising the following steps:

- selecting two prime numbers p and q which are distinct and of adjacent sizes;

- calculating the number n equal to the product p,q;

- calculating the lowest common multiple of the numbers (p-1) and (q-1): $\lambda(n)=LCM(p-1, q-1)$

- determining a number g, $0\leq g<n^2$, which satisfies the following two conditions during the calculation of a cryptogram c: $c=g^m \bmod n^2$:

a) g is invertible modulo n^2, and

b) $ord(g,n^2) = 0 \bmod n$,

the public key of the said device being formed by the parameters n and g and its private key being formed by the parameters p,q and $\lambda(n)$ or by the parameters p and q, a generation method characterised in that it consists in taking g=2, if g satisfies the said conditions a) and b).

2. A cryptographic communication system with public and private keys generated according to Claim 1, comprising a communication channel (20) and communicating devices (A, B), each device comprising at

least one communication interface (11), data processing means (10) and storage means (12, 13), characterised in that an encryption method is implemented in a first device (A) in order to send a number m representing a message, $0 \leq m < n$, to a second device (B), the said encryption method comprising the following steps:

- using the parameters of the public key (n_B, g_B) of the second device (B) in order to assign the values of the public key (n_B, g_B) to the parameters n and g,

- calculating the cryptogram $c = g^m \bmod n^2$,

the said cryptogram c then being transmitted over the communication channel to the second device.

3. A system according to Claim 2, characterised in that the device implementing the encryption method also comprises a generator (15) for a random integer number r, and in that the said device:

- performs the drawing of a random integer number r, and then

- calculates the cryptogram c by performing the following encryption calculation: $c = g^{m+nr} \bmod (n^2)$.

4. A system according to Claim 2, characterised in that the device implementing the encryption method also comprises a generator (15) for a random integer number r, and in that the said device:

- performs the drawing of a random integer number r, and then

- calculates the cryptogram c by performing the following encryption calculation: $c = g^m r^n \bmod (n^2)$.

5. A system according to Claim 4, characterised in that the second device (B) implements a decryption

method, in order to decrypt the said cryptogram c, and which comprises the performing of the calculation

$$m = \log_n(c^{\lambda(n)} \bmod n^2).\log_n(g^{\lambda(n)} \bmod n^2)^{-1} \bmod n$$

where $\log_n(x)=\frac{x-1}{n}$.

α being any integer

6. A system according to Claim 5, characterised in that a device (B) implementing the said decryption method precalculates the quantity:

$$\alpha_{n,g}=\log_n(g^{\lambda(n)} \bmod n^2)^{-1} \bmod n$$

and stores it secretly in the protected area of the program memory, x being any integer.

7. A system according to Claim 5, characterised in that, in one instance of the said decryption method, a device performs the following calculation steps, using the Chinese Remainder Theorem CRT:

$$m_p=\log_p(c^{p-1} \bmod p^2).\log_p(g^{p-1} \bmod p^2)^{-1} \bmod p.$$

$$m_q=\log_q(c^{q-1} \bmod q^2).\log_q(g^{q-1} \bmod q^2)^{-1} \bmod q.$$

$m=CRT(m_p,m_q,p,q)$, where $\log_p$ and $\log_q$ are such that

$$\log_i(x)=\frac{x-1}{i}$$

x being any integer.

8. A system according to Claim 7, characterised in that a device implementing the said decryption method precalculates the following quantities

$$\alpha_{p,g} = \log_p(g^{p-1} \bmod p^2)^{-1} \bmod p \text{ and}$$

$$\alpha_{q,g} = \log_q(g^{q-1} \bmod q^2)^{-1} \bmod q$$

and stores them secretly in the protected area of the program memory.

9. A cryptographic communication system with public and private keys generated according to Claim 1, comprising a communication channel (20) and communicating devices (A,B), each device comprising a communication interface (11), data processing means (10) and storage means (12, 13), characterised in that an encryption method is implemented in a first device (A) for sending a number m representing a message, $0 \leq m < n^2$, to a second device (B), the said encryption method comprising the following steps:

- using the parameters of the public key $K_B=(n_B,g_B)$ of the second device (B) in order to assign the values of the public key (n_B,g_B) to the parameters n and g,

- and performing the following calculations:

1. $m_1=m \bmod n$
2. $m_2=(m-m1)/n$
3. $c=g^{m1}\ m_2^n \bmod n^2$

the said cryptogram c being transmitted over the communication channel to the second device.

10. A system according to Claim 9, characterised in that the second device (B) receives the cryptogram c and implements a decryption method, in order to decrypt the said cryptogram which comprises the performance of the following calculation steps:

1. $m_1=\log_n(c^{\lambda(n)} \bmod n^2).\log_n(g^{\lambda(n)} \bmod n^2)^{-1} \bmod n$
2. $w=cg^{-m1} \bmod n$
3. $m_2=w^{1/n \bmod \lambda(n)} \bmod n$
4. $m = m_1 + nm_2$.

11. A system according to Claim 10, characterised in that a device implementing the said decryption method precalculates the following quantities:

$\alpha_{n,g}=\log_n(g^{\lambda(n)} \bmod n^2)^{-1} \bmod n$ and

$\gamma_n= 1/n \bmod \lambda(n)$

and stores them secretly in the protected area of the program memory.

12. A system according to Claim 10, characterised in that, in one instance of the said decryption method, a device performs the following calculation steps, using the Chinese Remainder Theorem:

1. $m_{1,p}=\log_p(c^{p-1} \bmod p^2)\log_p(g^{p-1} \bmod p^2)^{-1} \bmod p$
2. $w_p=cg^{-m1,p} \bmod p$
3. $m_{2,p}=w_p^{1/q \bmod p-1} \bmod p$
4. $m_{1,q}=\log_q(c^{q-1} \bmod q^2).\log_q(g^{q-1} \bmod q^2)^{-1} \bmod q$
5. $w_q=cg^{-m1,q} \bmod q$
6. $m_{2,q}=w_q^{1/p \bmod q-1} \bmod q$
7. $m_1=\mathrm{CRT}(m_{1,p},m_{2,p},p,q)$.
8. $m_2=\mathrm{CRT}(m_{1,q},m_{2,q},p,q)$.
9. $m = m_1 + pqm_2$ where $\log_p$ and $\log_q$ are such that $\log_i(x)=\frac{x-1}{i}$.

13. A system according to Claim 12, characterised in that, in one instance of the said decryption method, a device precalculates the following quantities:

$\alpha_{p,g}=\log_p(g^{p-1} \bmod p^2)^{-1} \bmod p$

$\alpha_{q,g}=\log_q(g^{q-1} \bmod q^2)^{-1} \bmod q$

$\gamma_p= 1/q \bmod p-1$

$\gamma_q= 1/p \bmod q-1$

and stores them secretly in the protected memory area of the program memory.

14. A system according to any one of Claims 10 to 13, in which the decryption method is used for calculating the signature s of a message m and the encryption method is used for verifying the said signature.

15. A cryptographic communication system with public and private keys generated according to Claim 1, comprising a communication channel (20) and communicating devices (A, B), each device comprising a communication interface (11), data processing means (10) and storage means (12, 13), characterised in that an encryption method is implemented in a first device (A) in order to send a number m representing a message, $0 \leq m < n$, to a second device (B), the said encryption method comprising the following steps:

- using the parameters of the public key $(n,g)_B$ of the second device (B) in order to assign the values of the public key (n_B, g_B) to the parameters n and g,

- calculating the cryptogram $c=g^m \bmod n^2$,

the said cryptogram c then being transmitted over the communication channel to the second device.

16. A system according to Claim 15, characterised in that the device implements the encryption method also comprising a generator (15) for a random integer number r, and in that the said device:

- performs the drawing of a random integer number r, and then

- calculates the cryptogram c, performing the following encryption calculation: $c=g^{m+rn} \bmod (n^2)$.

17. A system according to Claim 15 or 16, characterised in that the second device implements a method of decryption of the received cryptogram c, comprising the performance of the following calculation:

$m= \log_n(c^u \bmod n^2).\log_n(g^u \bmod n^2)^{-1} \bmod n$.

18. A method according to Claim 17, characterised in that a device implementing the said decryption method precalculates the quantity:

$\beta_{n,g}=\log_n(g^u \bmod n^2)^{-1} \bmod n$

and stores it secretly in the protected area of the program memory.

19. A system according to Claim 17, characterised in that, in one instance of the said decryption method, a device performs the following calculation steps, using the Chinese Remainder Theorem:

1. $m_p=\log_p(c^u \bmod p^2).\log_p(g^u \bmod p^2)^{-1} \bmod p$
2. $m_q=\log_q(c^u \bmod q^2).\log_q(g^u \bmod q^2)^{-1} \bmod q$
3. $m = CRT(m_p,m_q,p,q)$, where $\log_p$ and $\log_q$ are such that

$$\log_i(x)=\frac{x-1}{i}$$

x being any integer.

20. A system according to Claim 19, characterised in that a device implementing the said decryption method precalculates the following quantities:

$\beta_{p,g}=\log_n(g^u \bmod p^2)^{-1} \bmod p$

$\beta_{q,g}=\log_n(g^u \bmod q^2)^{-1} \bmod q$

and stores them secretly in the protected area of the program memory.

FIG.1

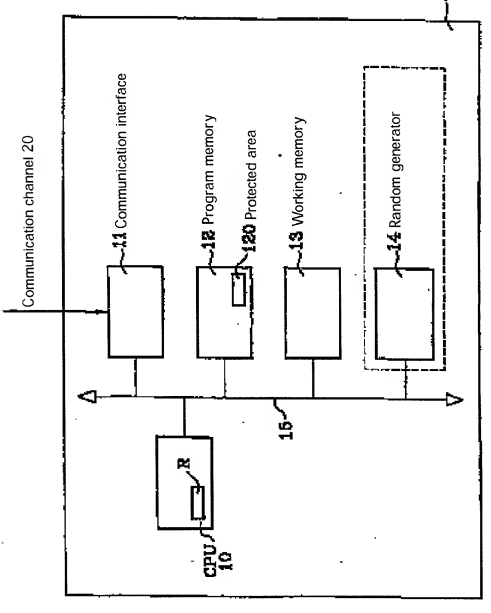

FIG.2

FIG.3

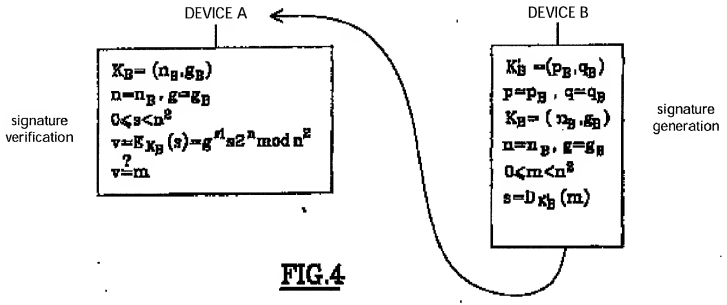

FIG.4

#3

COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY (Includes Reference to Provisional and International (PCT) Applications)	Attorney's Docket No. 032326-150

As a below named inventor, I hereby declare that:
My residence, post office address and citizenship are as stated below next to my name;
I BELIEVE I AM THE ORIGINAL, FIRST AND SOLE INVENTOR (IF ONLY ONE NAME IS LISTED BELOW) OR AN ORIGINAL, FIRST AND JOINT INVENTOR (IF PLURAL NAMES ARE LISTED BELOW) OF THE SUBJECT MATTER WHICH IS CLAIMED AND FOR WHICH A PATENT IS SOUGHT ON THE INVENTION ENTITLED:

PUBLIC AND PRIVATE KEY CRYPTOGRAPHIC METHOD

The specification of which (check only one item below):

☐ is attached hereto.

☒ was filed as United States Patent Application Number _____
on July 16, 2001
and was amended on _____ (if applicable).

☐ was filed as International (PCT) Application Number _____
on _____
and was amended on _____ (if applicable).

I HAVE REVIEWED AND UNDERSTAND THE CONTENTS OF THE ABOVE-IDENTIFIED SPECIFICATION, INCLUDING THE CLAIMS, AS AMENDED BY ANY AMENDMENT REFERRED TO ABOVE.

I ACKNOWLEDGE THE DUTY TO DISCLOSE TO THE U.S. PATENT AND TRADEMARK OFFICE ALL INFORMATION KNOWN TO ME TO BE MATERIAL TO PATENTABILITY AS DEFINED IN TITLE 37, CODE OF FEDERAL REGULATIONS, Sec. 1.56 (as amended effective March 16, 1992);

I do not know and do not believe the said invention was ever known or used in the United States of America before my or our invention thereof, or patented or described in any printed publication in any country before my or our invention thereof or more than one year prior to said application; that said invention was not in public use or on sale in the United States of America more than one year prior to said application; that said invention has not been patented or made the subject of an inventor's certificate issued before the date of said application in any country foreign to the United States of America on any application filed by me or my legal representatives or assigns more than six months prior to said application;

I hereby claim foreign priority benefits under Title 35, United States Code, §§ 119 (a)-(e) of any foreign application(s) for patent or inventor's certificate or of any International (PCT) Application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT International (PCT) Application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed:

PRIOR FOREIGN/PCT APPLICATION(S) AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. §119:

COUNTRY (If PCT, indicate "PCT")	APPLICATION NUMBER	DATE OF FILING (day, month, year)	PRIORITY CLAIMED UNDER 35 U.S.C. §119
France	99/00341	14 January 1999	☒Yes ☐No
			☐Yes ☐No
			☐Yes ☐No
			☐Yes ☐No
			Yes No

I hereby claim the benefit under Title 35, United States Code § 119(e) of any United States provisional application(s) listed below.

(APPLICATION NUMBER) (FILING DATE)

(APPLICATION NUMBER) (FILING DATE)

COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY (CONT'D) (Includes Reference to Provisional and International (PCT) Applications)	Attorney's Docket No. 032326-130

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States applications(s) or International (PCT) Application(s) designating the United States of America that is/are listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in that/those prior application(s) in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose to the U.S. Patent and Trademark Office all information known to me to be material to the patentability as defined in Title 37, Code of Federal Regulations § 1.56, which became available between the filing date of the prior application(s) and the national or international filing date of this application:

PRIOR U.S. APPLICATIONS OR INTERNATIONAL (PCT) APPLICATIONS DESIGNATING THE U.S. FOR BENEFIT UNDER 35 U.S.C. § 120:

U.S. APPLICATIONS			STATUS (check one)		
U.S. APPLICATION NUMBER	U.S. FILING DATE		PATENTED	PENDING	ABANDONED
			☐	☐	☐
PCT APPLICATIONS DESIGNATING THE U.S.					
PCT APPLICATION NO.	PCT FILING DATE	U.S. APPLICATION NUMBERS ASSIGNED (if any)			
PCT/FR99/02918	25 November 1999				

I hereby appoint the following attorneys and agent(s) to prosecute said application and to transact all business in the U.S. Patent and Trademark Office connected therewith and to file, prosecute and to transact all business in connection with international applications directed to said invention:

William L. Mathis	17,337	Eric H. Weisblatt	30,505	Bruce T. Wieder	33,815
Robert S. Swecker	19,885	James W. Peterson	26,057	Todd R. Walters	34,040
Platon N. Mandros	22,124	Teresa Stanek Rea	30,427	Ronni S. Jillions	31,979
Benton S. Duffett, Jr.	22,030	Robert E. Krebs	25,885	Harold R. Brown III	36,341
Norman H. Stepno	22,716	William C. Rowland	30,888	Allen R. Baum	36,086
Ronald L. Grudziecki	24,970	T. Gene Dillahunty	25,423	Brian P. O'Shaughnessy	32,747
Frederick G. Michaud, Jr.	26,003	Patrick C. Keane	32,858	Kenneth B. Leffler	36,075
Alan E. Kopecki	25,813	B. Jefferson Boggs, Jr.	32,344	Fred W. Hathaway	32,236
Regis E. Slutter	26,999	William H. Benz	25,952	Wendi L. Weinstein	34,456
Samuel C. Miller, III	27,360	Peter K. Skiff	31,917	Mary Ann Dillahunty	34,576
Robert G. Mukai	28,531	Richard J. McGrath	29,195		
George A. Hovanec, Jr.	28,223	Matthew L. Schneider	32,814		
James A. LaBarre	28,632	Michael G. Savage	32,596		
E. Joseph Gess	28,510	Gerald F. Swiss	30,113		
R. Danny Huntington	27,903	Charles F. Wieland III	33,096		

21839

and: ______________________________.

Address all correspondence to: James A. LaBarre
BURNS, DOANE, SWECKER & MATHIS, L.L.P.
P.O. Box 1404
Alexandria, Virginia 22313-1404

21839

Address all telephone calls to: James A. LaBarre at (703) 836-6620.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY (CONT'D) (Includes Reference to Provisional and International (PCT) Applications)	Attorney's Docket No. 032326-130

FULL NAME OF SOLE OR FIRST INVENTOR Pascal PAILLIER	SIGNATURE	DATE 29 August 2001
RESIDENCE (CITY & STATE/COUNTRY) 37 cours de Vincennes, 75020, Paris, FRANCE		CITIZENSHIP French
POST OFFICE ADDRESS (HOME ADDRESS) 37 cours de Vincennes, 75020, Paris, FRANCE		
FULL NAME OF SECOND JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE (CITY & STATE/COUNTRY)		CITIZENSHIP
POST OFFICE ADDRESS (HOME ADDRESS		
FULL NAME OF THIRD JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE (CITY & STATE/COUNTRY)		CITIZENSHIP
POST OFFICE ADDRESS (HOME ADDRESS		
FULL NAME OF FOURTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE (CITY & STATE/COUNTRY)		CITIZENSHIP
POST OFFICE ADDRESS (HOME ADDRESS		
FULL NAME OF FIFTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE (CITY & STATE/COUNTRY)		CITIZENSHIP
POST OFFICE ADDRESS (HOME ADDRESS		
FULL NAME OF SIXTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE (CITY & STATE/COUNTRY)		CITIZENSHIP
POST OFFICE ADDRESS (HOME ADDRESS		
FULL NAME OF SEVENTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE (CITY & STATE/COUNTRY)		CITIZENSHIP
POST OFFICE ADDRESS (HOME ADDRESS		
FULL NAME OF EIGHTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE (CITY & STATE/COUNTRY)		CITIZENSHIP
POST OFFICE ADDRESS (HOME ADDRESS		
FULL NAME OF NINTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE (CITY & STATE/COUNTRY)		CITIZENSHIP
POST OFFICE ADDRESS (HOME ADDRESS)		
FULL NAME OF TENTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE (CITY & STATE/COUNTRY)		CITIZENSHIP
POST OFFICE ADDRESS (HOME ADDRESS		